ORACLE

Oracle Cloud Infrastructure Security Architecture

2021年9月、第2.0版

目的の表明

このドキュメントは、Oracle Cloud Infrastructure (OCI)に組み込まれている機能と拡張機能の概要を示すものです。お客様がOCIのビジネス上の利点を評価し、ITプロジェクトを計画する際にお役立ていただくことのみを意図しています。

免責事項

このドキュメントには、ソフトウェアまたは印刷物などの形式を問わず、オラクルが独占的な権利を有する財産的情報が含まれています。この機密資料へのアクセスと使用は、オラクルとの間で締結され遵守に同意したオラクル・ソフトウェア・ライセンスおよびサービス契約の条件に従うものとします。このドキュメントとその内容の開示、コピー、複製および配布には、オラクルによる事前の承諾を必要とします。このドキュメントはライセンス契約の一部となるものではなく、オラクルおよびその子会社や関連会社との契約を構成するものではありません。

本文書は情報提供のみを目的として提供されており、記載されている製品機能の実装およびアップグレードを計画する際にお役立ていただくことのみを意図しています。マテリアルやコード、機能を提供することをコミットメント(確約)するものではないため、購買決定を行う際の判断材料になさらないで下さい。本書に記載されている機能の開発、リリース、および時期については、弊社の裁量により決定されます。製品アーキテクチャの性質により、コードの大幅な不安定化を招くリスクを冒さずに本書に記載されているすべての機能を安全に組み込むことは不可能な場合もあります。

改訂履歴

このドキュメントには、次の改訂が加えられています。

日付	改訂内容
2021年9月	Dedicated Region Cloud@Customerの情報を追加
2020年3月	初版発行

目次

概要 **4**

セキュリティ・ファーストの設計 **4**

第1世代のパブリック・クラウド 4

Oracle Cloud Infrastructure—次世代のパブリック・クラウド 4

プラットフォームのセキュリティ **4**

分離されたネットワーク仮想化 5

ハードウェア 5

物理ネットワーク 6

ネットワークのセグメント化 7

フォルトトレラントなインフラストラクチャ **8**

物理セキュリティ **8**

安全な接続 **9**

最小権限アクセス 9

複数の認証レイヤー 9

内部接続 9

外部接続 10

Dedicated Region Cloud@Customer **10**

運用上のセキュリティ **10**

防御的セキュリティ 10

攻撃的セキュリティ 11

セキュリティ保証 11

データとアプリケーションの保護 **11**

データへのアクセス 11

データの破壊 11

データの暗号化 12

APIのセキュリティ 12

信頼とコンプライアンスの文化 **12**

開発のセキュリティ 12

人員のセキュリティ 13

サプライ・チェーンのセキュリティ 13

コンプライアンス 13

監査 13

結論 **14**

参考資料 **14**

概要

Oracle Cloud Infrastructure (OCI)は、セキュリティ・ファーストの設計原則に基づいて設計された、次世代のInfrastructure-as-a-Service (IaaS)製品です。この原則は、分離されたネットワーク仮想化と、当初から変わらない物理ホスト・デプロイメントからなりますが、これらは従来のパブリック・クラウド設計では実現困難でした。この設計原則により、OCIはAPT攻撃から生じるリスクの軽減に貢献しています。

OCIは、データ・センターの物理ハードウェアからWebレイヤーまで及ぶ階層型の防御ときわめて安全な運用に支えられています。それに加えて、オラクルのクラウドには保護策と統制も用意されています。さらに、こうした保護策の多くはサードパーティ・クラウドやオンプレミス・ソリューションと連携し、現代のエンタープライズ・ワークロードとデータをそれぞれが存在する場所で保護するために一役買っています。

このドキュメントでは、クリティカルなワークロードや機微なワークロードを実行するお客様のセキュリティ要件にOCIがどのように対応しているかを説明します。OCIのプロビジョニング、使用、動作保証、保守を行うためのアーキテクチャ、データ・センター設計、人員の選定、プロセスにとって、セキュリティが不可欠である理由を詳しく述べます。

セキュリティ・ファーストの設計

クラウドの普及が進むなかで、セキュリティに関する懸念は重要性を増しています。Oracle Cloud Infrastructureは、その誕生以来、第1世代のクラウドから生じたセキュリティ上の問題の解決を最優先課題としてきました。

第1世代のパブリック・クラウド

第1世代のパブリック・クラウドは、仮想化とハイパーバイザの使用によって可能となったハードウェア・リソースの効率的な使用に重点を置いていました。こうしたクラウドは、プライベート・クラウドで使用されるのと同じテクノロジや原則の多くを基盤とし、高価なハードウェア・リソースを遊ばせておかないような設計を取っています。プライベート・データ・センターは境界防衛に頼っていたため、セキュリティはこの設計の基本原則とならないこともありました。パブリック・クラウドの使用が一般的になるとともに、ハイパーバイザの脆弱性に伴う攻撃に関する懸念も高まります。企業のお客様にとってセキュリティは主要な問題の1つであり、第1世代のパブリック・クラウドのハイパーバイザ設計に伴うリスクは増大の一途を辿っていました。

Oracle Cloud Infrastructure–次世代のパブリック・クラウド

OCIは、オラクルがエンタープライズのクリティカルなワークロード向けに開発したセキュリティ・ファーストのパブリック・クラウド・インフラストラクチャです。セキュリティ・ファーストとは、ハイパーバイザベースの攻撃によるリスクを軽減し、テナントの分離を強化するために、仮想化スタックを再設計したことを意味します。その結果、第1世代のクラウド・インフラストラクチャ設計よりもはるかに優れたセキュリティ上の効果をもたらす、次世代のパブリック・クラウド・インフラストラクチャ設計が生まれました。この設計は、すべてのデータ・センターとリージョンに実装されています。

OCIは完全なIaaSプラットフォームです。きわめて安全なホスティング環境でアプリケーションを構築、実行して、高いパフォーマンスと可用性を発揮するために必要なサービスを提供します。お客様は、ComputeサービスとDatabaseサービスを、お客様専用の物理サーバーであるベア・メタル・インスタンスで実行するか、ベア・メタル・ハードウェア上の分離コンピューティング環境である仮想マシン(VM)インスタンスとして実行することができます。ベア・メタル・インスタンスとVMインスタンスは同じタイプのサーバー・ハードウェア、ファームウェア、基盤ソフトウェアおよびネットワーキング・インフラストラクチャ上で実行されるため、どちらのインスタンス・タイプもOCIの保護策が各レイヤーに組み込まれています。

プラットフォームのセキュリティ

オラクルは、Oracle Cloud Infrastructureのアーキテクチャを、分離されたネットワーク仮想化、きわめて安全なファームウェア・インストール、制御された物理ネットワーク、およびネットワークのセグメント化を通じてプラットフォームのセキュリティを確保できるように設計しました。

分離されたネットワーク仮想化

OCI設計の中核をなすのが分離されたネットワーク仮想化で、ハイパーバイザによるリスクを大幅に軽減しています。

ハイパーバイザとは、クラウド環境内の仮想デバイスを管理し、サーバーとネットワークの仮想化を処理するソフトウェアです。従来の仮想化環境では、ハイパーバイザがネットワーク・トラフィックを管理し、VMインスタンス相互の間やVMインスタンスと物理ホストの間をトラフィックが流れるのを可能にしています。そのため、ハイパーバイザにおける複雑さと計算処理のオーバーヘッドは著しく増大します。VMエスケープ攻撃などのProof-of-Conceptコンピュータ・セキュリティ攻撃により、この設計がもたらす恐れのある重大なリスクが浮き彫りになりました。こうした攻撃は、攻撃者がVMインスタンスから「抜け出し」、基盤となるオペレーティング・システムにアクセスして、ハイパーバイザを支配できるようにすることで、ハイパーバイザの複雑さを悪用します。攻撃者がさらに他のホストにアクセスする可能性もありますが、こうした活動は時として検知されません。

OCIは、ネットワーク仮想化をハイパーバイザから切り離すことで、このようなリスクを軽減します。オラクルでは、ネットワーク仮想化を高度にカスタマイズされたハードウェアとソフトウェアのレイヤーとして実装しており、クラウドの制御はハイパーバイザとホストから分離され、専用のネットワーク上に配置されています。この強化され、監視されている制御レイヤーが、分離されたネットワーク仮想化を可能にしているのです。

分離されたネットワーク仮想化は、攻撃対象領域を制限することでリスクを軽減します。悪意のあるアクターが1つのホストでVMエスケープ攻撃に成功したとしても、クラウド・インフラストラクチャ内の他のホストには到達できません。攻撃はその1つのホストに効果的に封じ込められます。オラクルでは、分離されたネットワーク仮想化をすべてのリージョンのすべてのデータ・センターに実装しています。したがって、OCIのすべてのテナントがこの設計の恩恵を受けることになります。

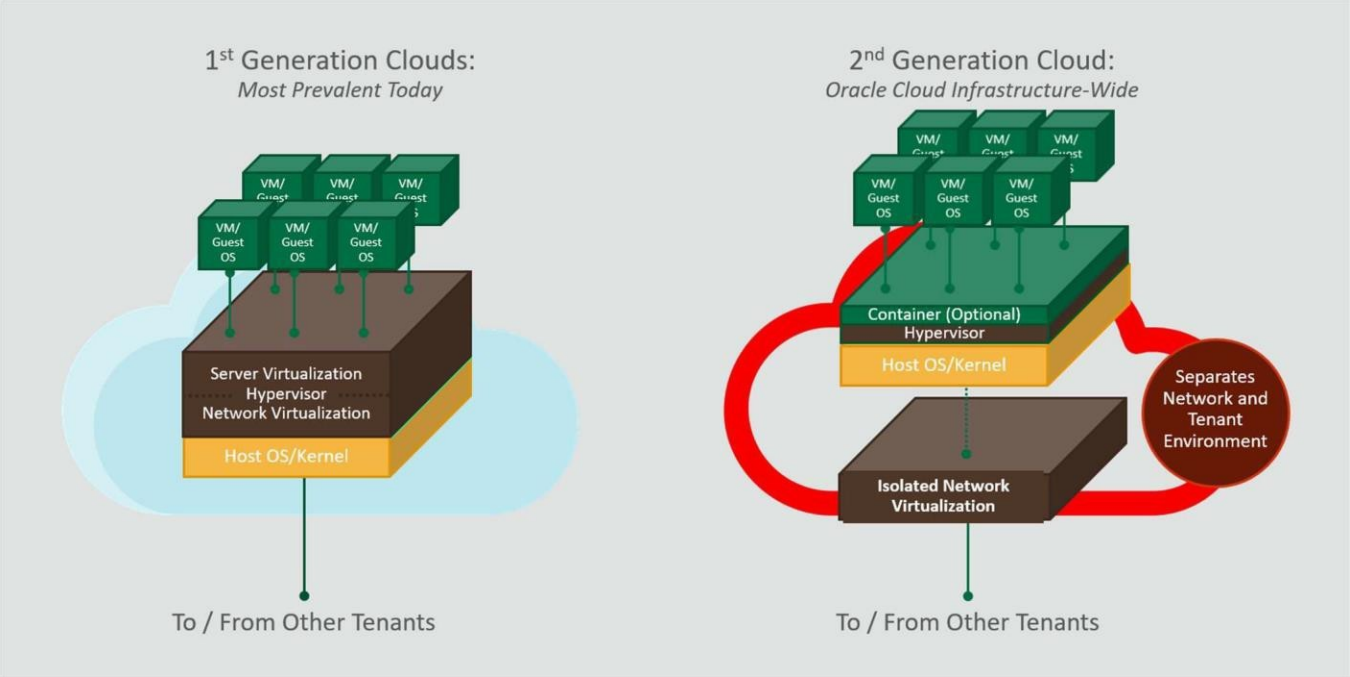

図1: 分離されたネットワーク仮想化により、オラクルの次世代クラウドのリスクを軽減

ハードウェア

OCIの主要な設計原則の1つは、ファームウェアベースの攻撃からテナントを保護することです。ファームウェア・レベルの脅威がますます広がりを見せるのに伴い、パブリック・クラウド・プロバイダにとっての潜在的なリスクが高まっています。オラクルでは、各サーバーがクリーンなファームウェアでプロビジョニングされるように、サーバーのファームウェアをワイプして再インストールするプロセスのためのハードウェアベースの信頼の基点（root of trust）を実装しました。このプロセスは、インスタンスのタイプにかかわらず、新しいサーバーが1つのテナントに対して、またはテナンシ間でプロビジョニングされるたびに使用されます。

ハードウェアベースの信頼の基点（root of trust）とは、オラクルの仕様に従って製造され、保護されたハードウェア・コンポーネントです。ファームウェアをワイプして再インストールするという特定のタスクの実行に限定されています。ハードウェアベースの信頼の基点（root of trust）は、ハードウェア・ホストの電源のオン/オフをトリガーし、既知のファームウェアのインストールを促し、予期したとおりにプロセスが完了したことを確認します。この方法でファームウェアをインストールすれば、永続的なサービス拒否(PDoS)攻撃や、ファームウェアにバックドアを仕込んでデータを盗んだり、他の方法でデータを利用できなくする試みなど、ファームウェアベースの攻撃によるリスクが軽減されます。さらに、内部サーバーはセキュア・ブートを使用するように構成されています。

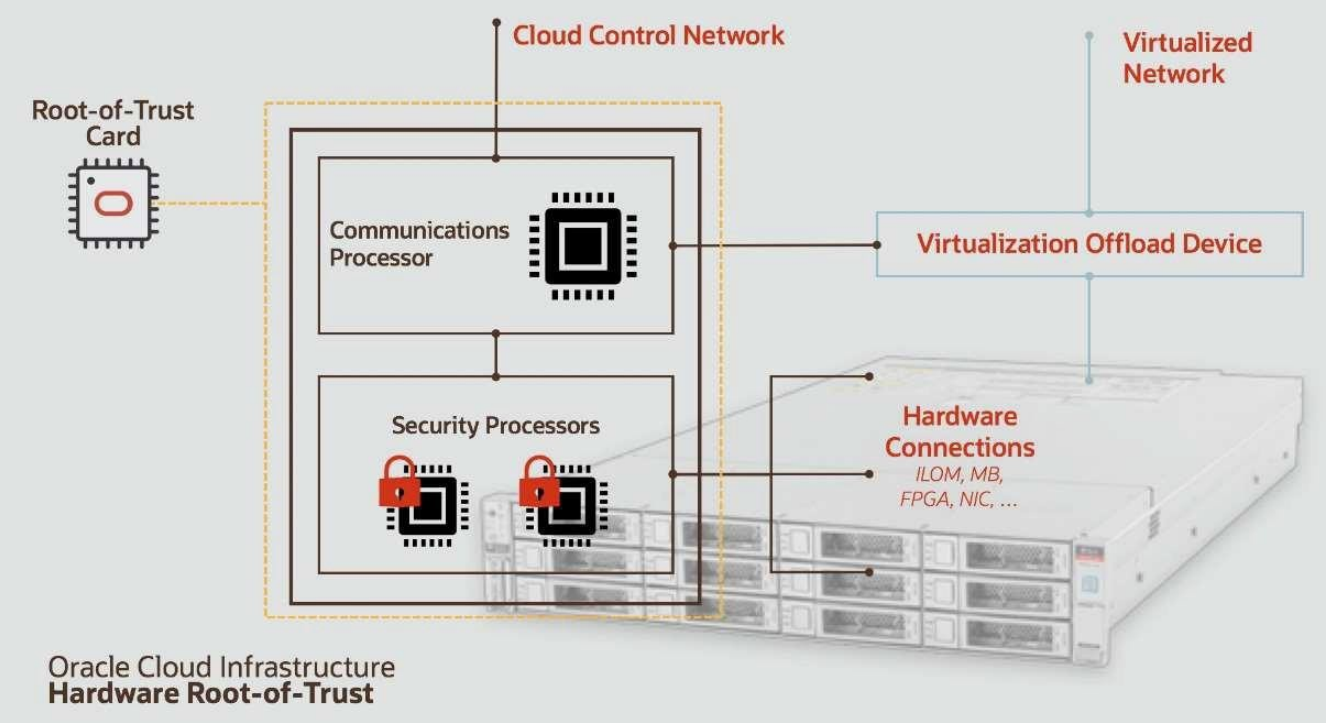

図2: ファームウェアのインストールに使用されるハードウェアベースの信頼の基点（root of trust）の設計

物理ネットワーク

OCIの物理ネットワーク・アーキテクチャは、お客様のテナンシをさらに分離し、脅威が拡大するリスクを抑えることで、ネットワーク仮想化に防御のレイヤーを追加します。物理ネットワークのコンポーネントは、OCIの物理レイヤーを形成するラック、ルーター、スイッチです。

Top-of-Rack (ToR)スイッチにはアクセス制御リスト(ACL)が適用されます。ACLは、トポロジ内の通信経路に従うことを強制します。たとえば、ToRスイッチは、仮想ネットワークのソースIPアドレスとそれに対応する物理ネットワーク・ポートが所定のマッピングに一致しないパケットをすべて破棄します。この不一致は、攻撃者が仮想ソースIPアドレスを偽装し、正当なトラフィック・ソースになりすまして他のテナントにアクセスしようとした場合に発生します。オラクルは、分離されたネットワーク仮想化デバイスの所定のIPアドレスを、デバイスが接続する物理ポートと関連付けることで、IPスプーフィングを防止できるようにACLを設計しました。さらに、接続先デバイスはパケットのリバースパス・チェックを実行し、カプセル化ヘッダーの改ざんに対処します。

物理レイヤーの設計は、仮想クラウド・ネットワーク(VCN)の仮想ポートに接続する、シンプルでフラットなネットワークです。この設計により、許可されたトラフィック・パスを管理する際の複雑さが軽減され、パスを迂回しようとする試みの可視性が向上します。

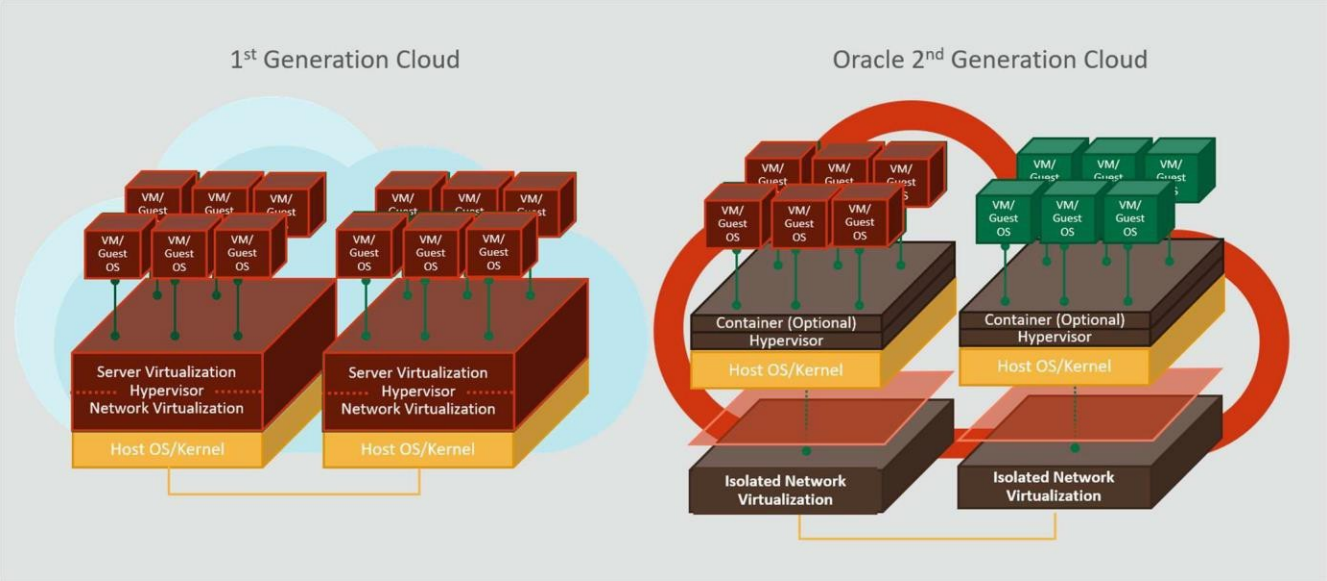

図3: シンプルでフラットなネットワーク設計により、次世代のクラウドを保護

ネットワークのセグメント化

オラクルは、OCIの物理ネットワークを、お客様とサービスを分離するように設計しました。このネットワークは、一意の通信プロファイルを持つエンクレーブにセグメント化されます。エンクレーブへのアクセスとエンクレーブからのアクセスは制御、監視されており、ポリシーに基づいています。

コンピュート・ホストの電源のオン/オフはIntegrated Lights Out Manager (ILOM)によって行われます。各ホストがILOMを1つ備え、他のホストとの直接の通信は禁止されています。ILOMネットワークは、OCIのコア・サービスがプロビジョニングされているサービス・エンクレーブからのみコマンド・メッセージを受け入れます。コア・サービスには、Networking、Identity and Access Management (IAM)、Block Volumes、Load Balancing、Auditなどがあります。オラクルの従業員がサービス・エンクレーブにアクセスするには、権限を持つ担当者によって付与された明示的なユーザー権限が必要です。このアクセスは定期的な監査とレビューの対象となります。サービス・エンクレーブはリージョンに対してローカルです。したがって、サービス・エンクレーブ間で必要なトラフィックは、インターネット・トラフィックと同じセキュリティ・メカニズム(インバウンドのSSH要塞ホストとアウトバウンドのHTTPSプロキシ)を通過します。

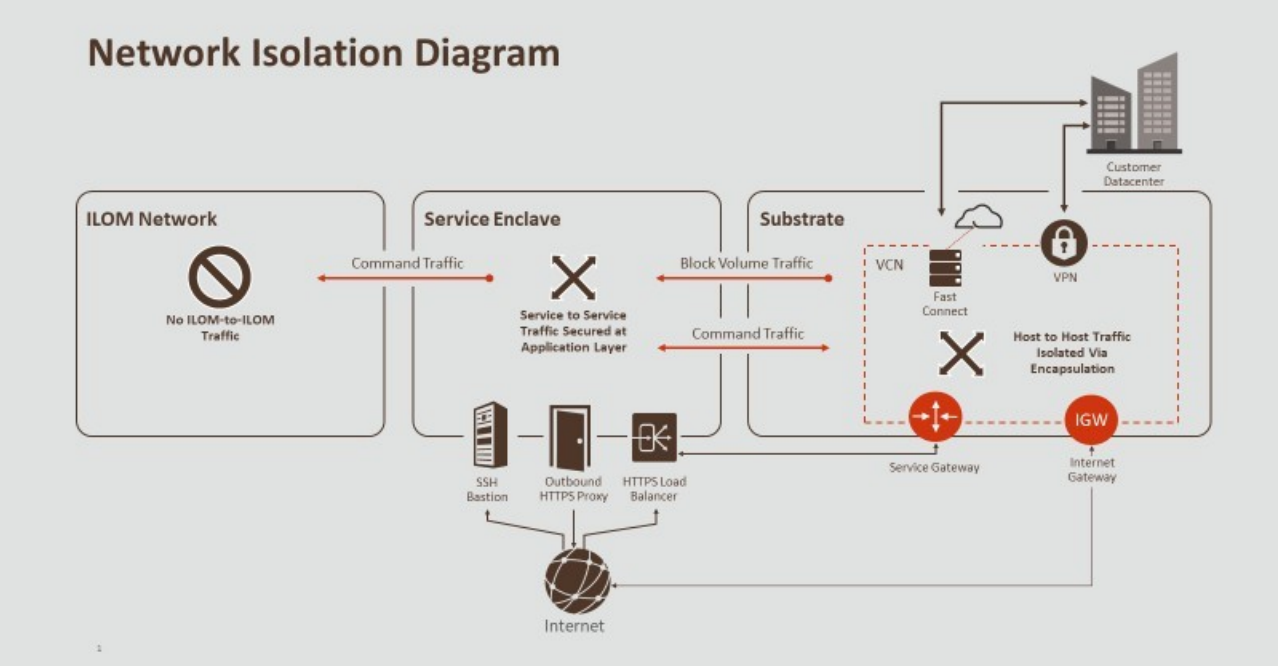

図4: ネットワークのセグメント化により、お客様のリソースとサービスを分離

フォルトトレラントなインフラストラクチャ

Oracle Cloud Infrastructureはリージョン単位で構成されており、リージョンは特定の地域内に構築されます。各リージョンには1つまたは2つ、あるいは3つの可用性ドメインがあり、各可用性ドメインは複数の障害ドメインに分割されます。お客様のインスタンスが位置するリージョンに可用性ドメインが1つあるのか複数あるのかにかかわらず、障害ドメインとリージョン間レプリケーションによるデータとサービスの回復性とバックアップのために、多数の冗長性レイヤーが用意されています。

サービスのアーキテクチャとデータ保管の仕組みにはフォルトトレランスが実装されています。サービスとデータは複数のハードウェア・ラックにまたがって存在し、それぞれのハードウェア・ラックにはノード・レベル、サーバー・レベル、ハードウェア・コンポーネント・レベルの複数の冗長性レイヤーが組み込まれています。接続とエッジ・サービスが各リージョンを他のリージョンやピア・ネットワークおよびお客様のデータ・センターと結び付けます。

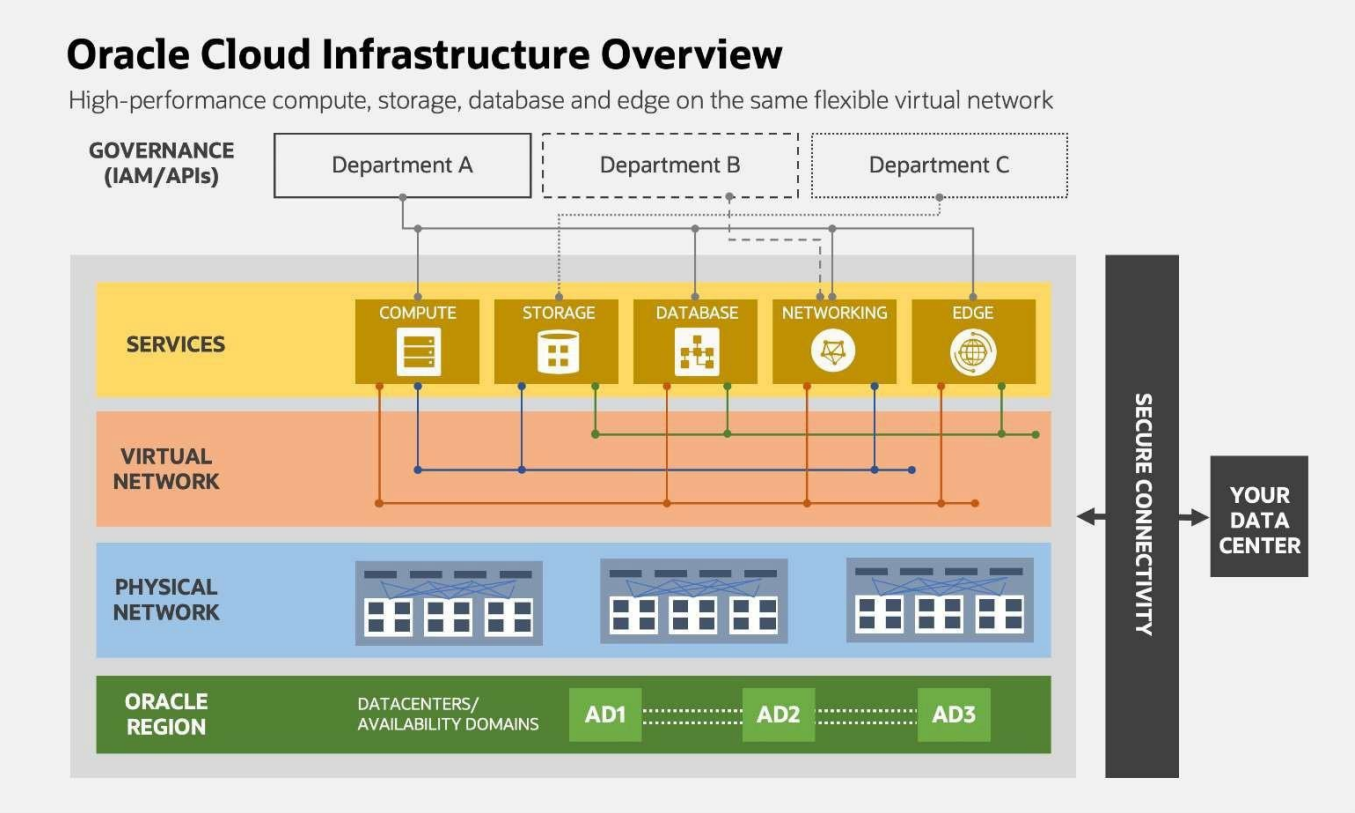

図5: OCIのリージョンにおけるフォルトトレラントな設計

物理セキュリティ

Oracle Cloud Infrastructureに対しては、候補となるデータ・センターやプロバイダ拠点を評価するためのリスク評価プロセスが実施されます。このプロセスでは、環境上の脅威、電力の可用性と安定性、ベンダーの評判と経歴、近隣施設の機能、地政学的な事情などの要素が考慮されます。

データ・センターはUptime InstituteとTelecommunications Industry Association (TIA)のANSI/TIA-942-A Tier 3またはTier 4標準に準拠し、クリティカルな機器運用に関するN2冗長性手法に従っています。OCIサービスを収容するデータ・センターは、冗長電源を使用し、発電機のバックアップを保持することが義務付けられています。オラクルでは、サーバー・ルームの気温と湿度を厳重に監視し、消火設備も完備しています。データ・センターのスタッフには、セキュリティや可用性に関する事象に対処できるように、イベント処理、インシデント対応およびエスカレーション手順の訓練を施しています。

データ・センターの物理セキュリティに対するオラクルの多層アプローチは建物自体から始まります。オラクルがパートナーの協力を得て建築するデータ・センター施設は、鋼鉄、コンクリートまたは同等の資材を用いることで耐久性が確保され、軽量車両の衝突による衝撃にも耐えるように設計されています。

データ・センターでは境界壁を使用してサイト外部を保護し、警備員と防犯カメラが車両の出入りを監視しています。データ・センターに立ち入る人は全員、サイト入口にあるセキュリティ・チェックポイントを通過しなければなりません。サイト固有のセキュリティ・バッジを持たない人は、政府発行の身分証明書を提示することと、申請書の承認を受けて建物へのアクセスを許可されていることの両方を求められます。すべての従業員と訪問者は、正式な身分証明バッジを見やすいように常時身に着けている必要があります。すべてのサイトに警備員が配置されています。

サイト入口とサーバー・ルームの間にある追加のセキュリティ・レイヤーは建物とリスク条件によって異なります。サーバー・ルーム自体は、カメラや2要素認証によるアクセス制御、侵入検知メカニズムなど、さらなるセキュリティ・レイヤーを備えることが義務付けられています。サーバー・ラックとネットワーキング・ラックの周囲には、床から天井までの物理的な障壁によって、分離されたセキュリティ・ゾーンが設けられています。この障壁は必要に応じて、上げ床の下から天井タイルの上まで及びます。サーバー・ルームへのアクセスはすべて、権限を持つ担当者の承認を受ける必要があり、必要な時間だけ許可されます。アクセスは監査の対象となります。また、システム内でプロビジョニングされたアクセスは定期的にレビューされ、必要に応じて更新されます。

安全な接続

オラクルでは、Oracle Cloud Infrastructure内のリソースや、OCIとお客様のオンプレミス・データ・センターの間のリソースに対する接続を制御し、保護しています。

最小権限アクセス

不要な権限は重大なリスクをもたらす恐れがあります。攻撃者が資格証明にアクセスする可能性もあり、攻撃者はその資格証明を利用してシステム中を動き回ります。過剰な権限を与えられたユーザーやアプリケーションから生じるリスクを軽減するために、オラクルでは、本番システムへのアクセス権を付与する際に*最小権限アクセス*の原則を用いています。承認されたサービス・チーム・メンバーのリストを定期的にレビューし、アクセス権に正当な必要性がない場合はアクセス権を取り消します。

本番システムにアクセスするには、多要素認証(MFA)が必要です。セキュリティ・チームがMFAトークンを発行し、アクティブでないメンバーのトークンは無効にします。オラクルでは、本番システムへのアクセスをすべてログに記録しており、ログはセキュリティ分析のために保管されています。

複数の認証レイヤー

脆弱なアカウント資格証明もクラウド環境に重大な脅威をもたらします。認証を強化するために、オラクルでは、複数のレイヤーからなる高度なアクセス制御を使用し、ネットワーク・デバイスやそれらのリソースをサポートするサーバーへのアクセスを制限しています。こうしたレイヤーの1つに、使用が義務付けられている、本番ネットワークへの仮想プライベート・ネットワーク(VPN)接続があります。このVPNは、パスワードの高度な多様性とUniversal 2nd Factor (U2F)認証を必要とします。U2Fとは、ハードウェア・キーを使用して2要素認証を強化し簡素化するオープン標準です。管理アクセスはすべてログに記録され、アクセス権限はすべて最小権限かどうかが監査されます。オラクルでは、認証に複数の要素を使用することで、攻撃者が脆弱なパスワードや漏えいしたパスワードで管理ネットワークにアクセスするのを防止しています。

内部接続

OCIの可用性ドメインとリージョンでは、他のOCIデータ・センターに転送されるクラウド・ネットワーク・トラフィックのデータ・プライバシーが保護されています。この保護は、MACsec (IEEE 802.1AE)暗号化によってさらに保護されている、プライベートの専用ワイド・エリア・ネットワーク(WAN)を使用した光ファイバー接続によって実現されます。MACsecとは、高速のレイヤー2ネットワーク暗号化プロトコルで、従来のレイヤー3暗号化ではカバーされない可能性がある、他のnon-IPレイヤー3プロトコルのトラフィック(DNSやICMPなど)を暗号化します。

外部接続

お客様は、OCIテナンシからキャンパス、プライベート・データ・センター、または他のクラウドへの接続が必要になることがよくあります。オラクルでは、OCIをプライベートVCNと非VCNネットワークに安全に接続する方法を2つ用意しています。

- **サイト間VPN:** パブリック・インターネット経由でのルーティングが可能な、暗号化された専用トンネル
- **FastConnect:** プライベートの専用高速WAN接続。オプションでIPSec VPNトンネルを使用可能

Dedicated Region Cloud@Customer

オラクルは、Dedicated Region Cloud@Customerも提供しています。これは、Autonomous DatabaseやOracleクラウド・アプリケーションをはじめとするオラクルの次世代クラウド・サービスのすべてをお客様のデータ・センターで利用できるようにするクラウド・リージョンです。オラクルでは、Dedicated Region Cloud@Customerリージョンを、Oracle Cloud Infrastructureの他の部分と同じセキュリティ・ファーストの設計原則に基づいて構築しています。さらに、この専用リージョンをお客様のデータ・センターに提供し、セキュリティやコンプライアンス、法規制の厳しい要件にも対処できるよう支援しています。このモデルでは、お客様のデータをお客様のサイトに保管することで、レイテンシやデータに関する現地の要件に対処しているほか、お客様がデータのバックアップとリカバリを管理できます。

Dedicated Region Cloud@Customerリージョンはお客様のデータ・センターにデプロイされるため、Oracle Dedicated Region Cloud@Customerシステム関連の物理セキュリティ、ネットワーク接続、アクセス制御はお客様が管理する必要があります。コントロール・プレーン操作(たとえば、起動、停止、終了などの操作)も含め、お客様のデータはオンプレミスにとどまり、リージョンから流出することはありません。

運用上のセキュリティ

オラクルは、Oracle Cloud Infrastructureのセキュリティ確保に専任で従事する大規模なセキュリティ専門部隊を擁しています。この部隊の中で、いくつかのチームが安全な開発、監視、テストや、規制および認証プログラムへの確実なコンプライアンスについて責任を負っています。

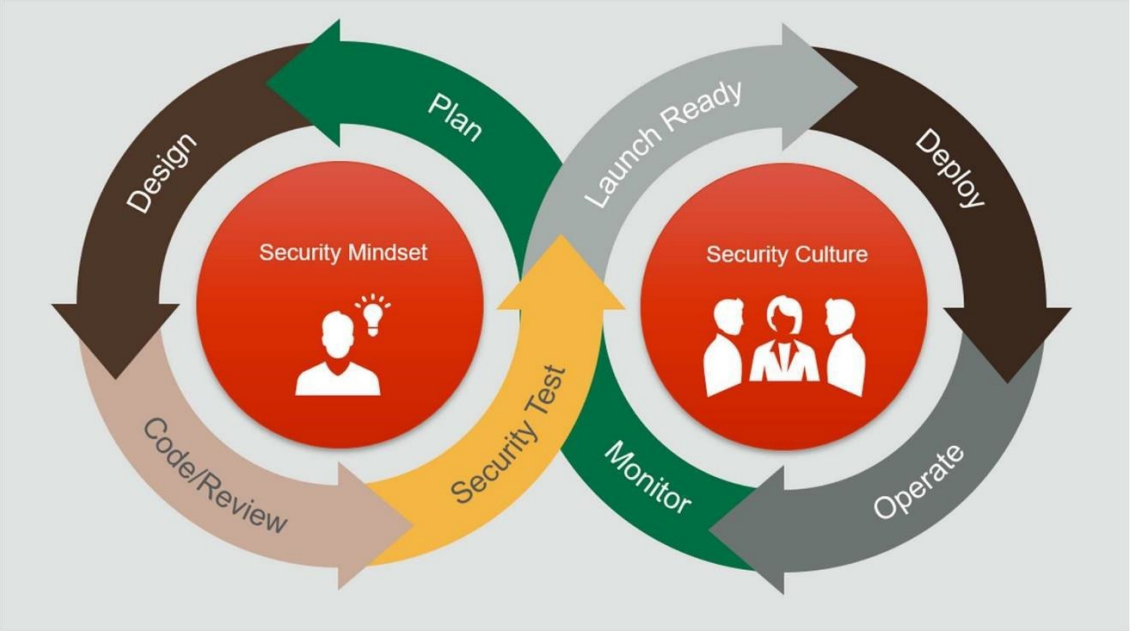

図6: OCIにおける運用上のセキュリティのフロー

防御的セキュリティ

いかなるコンピューティング環境においても、ネットワーキング・インフラストラクチャやコンピュート・インフラストラクチャに対する攻撃は日常的に発生する可能性があります。OCIでは、防御の専門家とアナリストからなる専任チーム(防御的セキュリティ・チーム)がこうした事象を監視し、対応しています。このチームのメンバーはクラウド・セキュ

リティの初動対応要員です。彼らは、絶えず先回りしてOCI内の潜在的脅威を発見し、OCIのサービス・エンクレーブ内のエクスプロイト経路を遮断します。チームがインシデントを検出すると、最新のセキュリティ運用手法とDevSecOps対応の構成およびツールを使用して、インシデントを速やかに修正すべく作業にあたります。

オラクルのチームは、お客様のテナンシにおける脅威の監視は行いません。テナンシへのセキュリティ侵害インジケータを監視してセキュリティ事象に対処することの責任は、お客様が負います。

攻撃的セキュリティ

OCIのセキュリティ・アーキテクチャの新機能が開発または変更された後、それがセキュリティ・ベンチマークを満たしていることを攻撃的セキュリティ・チームが検証します。このチームの任務は、攻撃者(巧妙な不正アクターや国民国家を含む)が用いる方法を理解し、模倣することです。この取り組みには、研究やペネトレーション・テスト、Oracleのハードウェアおよびソフトウェアに対する高度な脅威のシミュレーションが含まれます。攻撃的セキュリティ・チームの取り組みは、安全な開発や安全なアーキテクチャ、防御機能に幅広く反映されています。

セキュリティ保証

オラクルでは、既存のオラクルおよび業界の標準に即した高度なセキュリティ標準を含むセキュリティ計画を策定し、実施しています。クラウド・プラットフォームのセキュリティを確保するために、セキュリティ保証グループがサービス・チームやオラクル全社のセキュリティおよびリスク関係者と協力して、OCIを構築し運用するチームとOCIを基盤とするチーム向けのセキュリティ統制、テクノロジ、プロセス、ガイダンスを策定し、展開します。

データとアプリケーションの保護

オラクルは、Oracle Cloud Infrastructureのデータ処理および管理プラクティスを、お客様がデータの構成とツールの提供を通じて自社のデータとアプリケーションを外部の脅威から保護できるように設計しました。

データへのアクセス

オラクルでは、お客様とのやり取りにおいて、大きく分けて2種類のデータを定義しています。

- **お客様に関するデータ:** OCIアカウントの運用とサービスの料金請求に必要な連絡先と関連情報。オラクルがアカウント管理の目的で収集する個人情報の使用は、Oracle General Privacy Policyに従います。
- **お客様が保管するデータ:** お客様がOCIに保管するファイル、ドキュメント、データベースなどのデータ。オラクルによるこのデータの扱いについては、Oracle Services Privacy PolicyとData Processing Agreement for Oracle Servicesに記載されています。

データの破壊

オラクルでは、廃棄したハードウェアにデータが残ることのないように、物理的な破壊と論理的なデータ消去のプロセスを使用しています。

ストレージ・メディアの破壊

Oracle Asset Managementの要件では、お客様のデータが含まれているストレージ・メディアを、それが保管されているデータ・ホールから持ち出すことを明確に禁止しています。データ・センター内の各データ・ホールには、安全なメディア処分容器があります。ハード・ディスクやその他のストレージ・メディアが故障した場合や、処分のために本番システムから取り外された場合には、この安全な容器に入れて、消磁と細断が行われるまで保管します。

データの消去

お客様がVMインスタンスを解放すると、APIコールによって、そのインスタンスを削除するワークフローが開始されます。新しいベア・メタル・コンピュート・インスタンスがサービスに追加されるか、お客様またはサービスによって解放されると、ハードウェアが解放されて再割当てのためにインベントリに戻る前に、プロビジョニング・ワークフローがハードウェアに対して実行されます。この自動ワークフローでは、ホストに接続されている物理メディアが検出されます。次に、メディア・タイプに適した消去コマンドが実行されて、安全な消去が開始されます。

お客様による使用を意図したホストには、お客様のストレージ・ボリュームのキャッシュに使用されるネットワーク接続ストレージもあります。このディスクは、AT Attachment (ATA)セキュリティ消去コマンドを使用して消去されます。消去プロセスが完了すると、ワークフローにより、BIOSをフラッシュし、ドライバを更新し、ハードウェアを既知の良好な状態に戻すプロセスが開始されます。ハードウェアに障害がないかどうかのテストも行われます。ワークフローが失敗するか、障害が検出された場合、そのホストにはさらなる調査のためのフラグが立てられます。

お客様がブロック・ストレージ・ボリュームを終了すると、鍵が取消不可能な方法で削除され、データは完全にアクセス不可になります。

データの暗号化

OCIでは、すべてのデータをあらゆる場所で常に暗号化することを目標に掲げた「ユビキタス暗号化」プログラムを導入する取り組みを進めています。お客様のテナントのデータには、保存時と転送中のいずれにおいても暗号化を使用します。Block VolumesサービスとObject Storageサービスでは、256ビット暗号化によるAdvanced Encryption Standard (AES)アルゴリズムを使用することで、保存データの暗号化がデフォルトで可能になっています。転送中のコントロール・プレーン・データは、Transport Layer Security (TLS) 1.2以上を使用して暗号化されます。

APIのセキュリティ

最新のクラウド環境では、APIはアプリケーションの機能に不可欠ですが、その一方で、攻撃対象領域を広げる原因にもなっています。オラクルは、クラウド環境のアプリケーションにとってAPIのセキュリティが重要であることを認識し、そのセキュリティを提供するAPI Gatewayサービスを開発しました。

API Gatewayは、OCI上のお客様のネットワークと統合される、フルマネージド型のリージョン単位のサービスです。APIゲートウェイにより、お客様はパブリックまたはプライベートのAPIを公開し、クライアントから受信したリクエストを処理し、セキュリティ、可用性および検証のポリシーを適用することができます。さらに、APIゲートウェイはバックエンド・サービスにリクエストを転送し、バックエンド・サービスからのレスポンスにポリシーを適用した後、レスポンスをクライアントに転送することもできます。APIゲートウェイはバックエンド・サービスを保護、分離し、お客様がAPIコールを計測できるよう支援します。

クライアントからAPIゲートウェイへの接続では、常にTLSを使用してデータの機密性と完全性を維持しています。また、APIゲートウェイからバックエンド・サービスへの接続でTLSを使用するようにお客様が構成することもできます。

信頼とコンプライアンスの文化

オラクル全社に広がる信頼とコンプライアンスの文化は、Oracle Cloud Infrastructureにおけるすべてのプラクティスに浸透しています。

開発のセキュリティ

Oracle Software Security Assurance (OSSA)は、製品がお客様によってオンプレミスで使用されるのか、Oracle Cloudを通じて提供されるのかに関係なく、製品の設計、構築、テストおよび保守にセキュリティを組み込むオラクルの手法です。オラクルの目標は、費用対効果の高い自らの体験を提供しながらお客様がセキュリティ要件を満たせるように支援することです。業界をリードするOSSAの標準、テクノロジ、プラクティスには、次の目標があります。

- **セキュリティ・イノベーションを促進する:** オラクルの長年にわたるセキュリティ・イノベーションの伝統は、ハイブリッドのクラウド・データ・センター全体にわたって一貫したセキュリティ・ポリシーを導入、管理することを可能にするソリューションに受け継がれています。こうしたソリューションには、データベースのセキュリティおよびアイデンティティ管理やセキュリティの監視およびアナリティクスなどがあります。
- **すべてのOracle製品でセキュリティの脆弱性を軽減する:** OSSAプログラムには、オラクルのセキュア・コーディング基準、開発部門に義務付けられているセキュリティ・トレーニング、開発グループ内でのセキュリティ・リーダーの育成、自動化された分析ツールやテスト・ツールの使用などが含まれています。

- **リリース済の製品におけるセキュリティ脆弱性の影響を軽減する:** オラクルでは、セキュリティ脆弱性の開示と修正に関して、透明性の高いポリシーを採用しています。すべてのお客様に平等に対処し、Critical Patch Updateプログラムや Security Alertプログラムを通じて有効なセキュリティ・パッチの提供に取り組んでいます。

人員のセキュリティ

オラクルは、最も優れた候補者を雇用し、従業員の能力を伸ばすことを目指しています。オラクルでは、すべての従業員を対象とした基本的なセキュリティ・トレーニングのほか、最新のセキュリティ技術やエクスプロイト、方法論について学ぶ専門的なトレーニング・コースを提供しています。情報セキュリティとプライバシーに関するプログラムを網羅した全社的な標準トレーニング・プログラムも用意しています。さらに、オラクルは各種業界団体に参加するとともに、従業員を専門家向けのカンファレンスに派遣し、他の業界エキスパートと協力しながら新たな課題に取り組んでいます。オラクルのセキュリティ・トレーニング・プログラムの目的は、従業員がお客様と製品を保護できるよう支援すること、セキュリティ分野に関する従業員の関心を強化しつつ、優秀な人材を確保・維持するというミッションを推進することです。

オラクルは、高い倫理観と優れた判断力を持つ人々の雇用にも努めています。すべての従業員に対して、犯罪歴の調査や、国内の採用ルールに即した雇用前審査など、法律で許可されたスクリーニングが雇用前に実施されます。オラクルでは、優れた業績を認識し、成長の機会を特定するために、業績評価プロセスを管理しています。セキュリティはチーム評価プロセスの1要素として使用されます。このアプローチにより、オラクルのセキュリティ標準に関するチームのパフォーマンスを可視化し、重要なセキュリティ・プロセスに必要なベスト・プラクティスと改善の余地を見きわめることができます。

サプライ・チェーンのセキュリティ

オラクルには、エンタープライズクラスの安全なハードウェアを開発してきた長い歴史があります。OCIサービスの提供に使用されるハードウェアのセキュリティは、ハードウェア・セキュリティ・チームが設計し、テストしています。このチームはサプライ・チェーンと連携し、ハードウェア・コンポーネントをオラクルの厳しいハードウェア・セキュリティ標準に照らして検証します。

コンプライアンス

オラクルは、お客様がセキュリティとコンプライアンスのニーズに的確に対応できるようサービスの提供に投資を続けています。独立した保証により、信頼を促進し、サードパーティ・サービス・プロバイダとの関係における強い信頼を構築しています。この信頼と信用を得るために、オラクルは多くの定期的プログラムを通じて、グローバルな認証、地域や業界固有の認証へのコンプライアンスを維持し、そのコンプライアンスを証明するレポートを発行しています。こうしたレポートは、お客様の内部コーポレート・ガバナンス、リスク管理プロセス、ベンダー管理プログラム、規制監督において重要な役割を果たすことがあります。さらに、クラウド・ネイティブのDevOpsテクノロジにより、サービス・デプロイメントの自動化を利用することで、オラクルは世界中のリージョンのサービス・コンプライアンスを統合することができます。

監査

オラクルでは、OCI、プラットフォーム、アプリケーションに対し、ペネトレーション・テスト、脆弱性テスト、セキュリティ評価を定期的に実施しています。これらのテストの目的は、OCIサービスのセキュリティ全般を検証し、改善することです。

オラクルでは、各国のデータ保護の法律、規制、業界標準に関連したセキュリティ、機密性および可用性の統制について、外部の監査機関や評価機関に検査を依頼し、意見を求めています。

また、クラウド・セキュリティ・テスト・ポリシーで概説されているように、お客様自身による、または第三者によるテナンシのテストを実施することを許可しています。

結論

Oracle Cloud Infrastructureは、クリティカルなワークロードのセキュリティをオラクルの次世代パブリック・クラウドの中心に据えています。財務アプリケーションやシチズンサービス・アプリケーションなど、セキュリティ重視のワークロードを実行するお客様向けに、Oracle Cloud Infrastructureは、第1世代のクラウドに一般的に関連する攻撃面やリスクを軽減するセキュリティ・ファーストのアーキテクチャを提供します。オラクルは、アーキテクチャ、データ・センター設計、人員の選定およびOracle Cloud Infrastructureのプロビジョニング、使用、動作保証、保守のプロセスにセキュリティ機能とセキュリティ統制を組み込んでいます。Oracle Cloud Infrastructureは、最も高度なセキュリティ要件を伴う世界で最もクリティカルなデータ向けに構築された最新のパブリック・クラウドです。

参考資料

- Oracle Corporate Security Practices
- Oracle Cloud Compliance
- Oracle Software Security Assurance (OSSA)
- Oracle Security Testing Policy
- Oracle Cloud Infrastructureのセキュリティの詳細